DT05 Rec'd PCT/PTO 0 6 DEC 2004

DESCRIPTION

HIGH-DENSITY OPTICAL DISC, METHOD FOR RECORDING AND REPRODUCING ENCRYPTED DATA THEREON

1. Technical Field

The present invention relates to a high-density optical disc from which data can be reproduced, a method for encrypting data and recording the encrypted data thereon, and a method for reproducing the encrypted data recorded thereon.

2. Background Art

Recently, large-capacity digital versatile discs (DVDs) capable of permanently storing high-quality video and audio in comparison with compact discs (CDs) have been developed, commercialized and supplied. Types of the DVDs include a DVD-read only memory (DVD-ROM), a write once DVD recordable (DVD-R), a DVD-random access memory (DVD-RAM) or DVD rewritable (DVD-RW), etc.

Standardization of a high-density rewritable optical disc, e.g., a Blu-ray disc rewritable (BD-RE), capable of recording high-density data, is ongoing. The BD-RE will be described in detail.

Fig. 1 shows recording unit blocks (RUBs) of a high-density rewritable optical disc, e.g., a Blu-ray disc rewritable (BD-RE). As shown in Fig. 1, a single RUB consisting of a run-in area, physical cluster area and run-out area or a sequence of RUBs consisting of run-in areas, physical cluster areas, run-out areas and the third guard area (Guard_3) located in a tail of the sequence of RUBs can be recorded in a BD-RE 100. In the sequence of the RUBs, each RUB consisting of the run-in area,

the physical cluster area and the run-out area can be repeated twice or more.

As shown in Fig. 2, the run-in area includes the first guard area (Guard_1) and a preamble area (PrA). The preamble area includes the first synchronous data (Sync_1) and the second synchronous data (Sync_2). The first synchronous data and second synchronous data include 24-bit synchronous body data and a 6-bit synchronous ID, respectively.

The first and second synchronous data items are discriminated by different unique synchronous IDs. For example, the first synchronous data has a value of "000 100" as the synchronous ID. The second synchronous data has a value of "010 000" as the synchronous ID.

As shown in Fig. 3, the run-out area can include a post-amble area (PoA) and the second guard area (Guard_2). The post-amble area contains the third synchronous data (Sync_3). The third synchronous data includes 24-bit synchronous data and a 6-bit synchronous ID. The 6-bit synchronous ID of the third synchronous data is different from the 6-bit synchronous IDs of the first and second synchronous data. For example, the 6-bit synchronous ID of the third synchronous data has a value of "000 001".

The video and audio data recorded in the physical cluster area are read in synchronization with the synchronous data recorded in the run-in and run-out areas. Then, the video and audio data are reproduced as original video and audio signals through a reproduction signal processor such as a moving picture experts group (MPEG) decoder.

As shown in Fig. 4, the physical cluster area can contain a data stream associated with video data of moving pictures and audio data, frame synchronous information, a long distance error correction (LDC) code, a burst indicator sub-code (BIS) and an address unit (AU).

The LDC code and BIS are recorded on the basis of well-known

Reed-Solomon code words for error correction. The AU is used for correctly searching for a position of recorded data. As shown in Fig. 5, the physical cluster area contains 16 AUs (AU 0 ~ AU 15). An AU of 9 bytes includes address unit (AU) number information, flag bits, etc. The flag bits are reserved and set to "00h".

As shown in Fig. 6, the AU numbers are linked to physical sector numbers and also linked to physical address in pre-groove (ADIP) addresses. The AU number is useful as reference information in searching for the position of recorded data.

Thus, an optical disc apparatus such as a BD-RE recorder, etc. reads and confirms the physical sector numbers and physical ADIP addresses linked to the AU numbers. Then, the optical disc apparatus searches for a video and audio data stream recorded in the physical cluster area and then reads the searched data stream. Then, the optical disc apparatus performs an MPEG decoding operation to reproduce and output original video and audio signals.

Recently, it has been expected that the high-density optical disc, e.g. the BD-ROM, corresponding to the high-density rewritable optical disc will be developed. The high-density optical disc such as the BD-ROM must be able to maintain reproduction compatibility with a high-density rewritable optical disc such as a BD-RE on which data is recorded in a discontinuous recording format and must be able to prevent unauthorized or unlawful usage. However, there is not yet provided a method for effectively maintaining the above-described reproduction compatibility and preventing the unauthorized or unlawful usage.

3. Disclosure of Invention

Therefore, it is an object of the present invention to provide a high-density optical disc, a method for encrypting data and recording the encrypted data thereon, and a method for reproducing the encrypted data recorded thereon, which can

maintain reproduction compatibility with a high-density rewritable optical disc such as a BD-RE on which data is recorded in a discontinuous recording format, can encrypt the data so that unauthorized or unlawful usage can be prevented, and can record and reproduce the encrypted data.

In accordance with one aspect of the present invention, the above and other objects can be accomplished by the provision of a high-density optical disc, wherein data is encrypted, and the encrypted data is recorded in the data recording area according to a discontinuous recording format.

In accordance with another aspect of the present invention, there is provided a high-density optical disc, wherein data is encrypted on the basis of synchronous data recorded in the data recording area, and the encrypted data is recorded in the data recording area according to a discontinuous recording format.

In accordance with another aspect of the present invention, there is provided a high-density optical disc, wherein data is encrypted on the basis of address unit number information recorded in the data recording area, and the encrypted data is recorded in the data recording area according to a discontinuous recording format.

In accordance with another aspect of the present invention, there is provided a high-density optical disc, wherein data is encrypted on the basis of disc radius information recorded in the data recording area, and the encrypted data is recorded in the data recording area according to a discontinuous recording format.

In accordance with another aspect of the present invention, there is provided a method for encrypting data and recording the encrypted data on a high-density optical disc, comprising the steps of: (a) encrypting data on the basis of synchronous data recorded on the high-density optical disc; and (b) recording the encrypted data in a discontinuous recording format.

In accordance with another aspect of the present invention, there is provided a method for encrypting data and recording the encrypted data on a high-density optical disc, comprising the steps of: (a) encrypting data on the basis of address unit number information recorded on the high-density optical disc; and (b) recording the encrypted data in a discontinuous recording format.

In accordance with another aspect of the present invention, there is provided a method for encrypting data and recording the encrypted data on a high-density optical disc, comprising the steps of: (a) encrypting data on the basis of disc radius information recorded on the high-density optical disc; and (b) recording the encrypted data in a discontinuous recording format.

In accordance with another aspect of the present invention, there is provided a method for reproducing encrypted data recorded on a high-density optical disc, comprising the steps of: (a) searching for and reading synchronous data recorded on the high-density optical disc; (b) decrypting encrypted data on the basis of the read synchronous data; and (c) decoding the decrypted data to original signal, and reproducing and processing the original signal.

In accordance with another aspect of the present invention, there is provided a method for reproducing encrypted data recorded on a high-density optical disc, comprising the steps of: (a) searching for and reading address unit number information recorded on the high-density optical disc; (b) decrypting encrypted data on the basis of the read address unit number information; and (c) decoding the decrypted data to original signal, and reproducing and processing the original signal.

In accordance with yet another aspect of the present invention, there is provided a method for reproducing encrypted data recorded on a high-density optical disc, comprising the

steps of: (a) searching for and reading disc radius information recorded on the high-density optical disc; (b) decrypting encrypted data on the basis of the read disc radius information; and (c) decoding the decrypted data to original signal, and reproducing and processing the original signal.

4. Brief Description of Drawings

The accompanying drawings, which are included to provide a further understanding of the invention, illustrate the preferred embodiments of the invention, and together with the description, serve to explain the principles of the present invention.

Fig. 1 is a view illustrating recording unit blocks (RUBs) of a Blu-ray disc rewritable (BD-RE);

Fig. 2 is a view illustrating the configuration of a run-in area contained in an RUB of the BD-RE;

Fig. 3 is a view illustrating the configuration of a run-out area contained in the RUB of the BD-RE;

Fig. 4 is a view illustrating an address unit number (AUN) and data stream recorded in the physical cluster area;

Fig. 5 is a view illustrating an address unit (AU) recorded in the physical cluster area of the BD-RE;

Fig. 6 is a view illustrating relations between a physical sector number, an address unit number and a physical address in pre-groove (ADIP) address associated with the BD-RE;

Fig. 7 is a view illustrating the configuration of a run-in area contained in an RUB of a Blu-ray disc-read only memory (BD-ROM) in accordance with the first embodiment of the present invention;

Fig. 8 is a view illustrating the configuration of a run-out area contained in the RUB of the BD-ROM in accordance with the first embodiment of the present invention;

Fig. 9 is a view illustrating the relationship between an encoding system to which an encryption and recording method is applied, and the BD-ROM in accordance with the first embodiment

of the present invention;

Fig. 10 is a view illustrating the relationship between an encoding system to which an encryption and recording method is applied, and the BD-ROM in accordance with the second embodiment of the present invention;

Fig. 11 is a view illustrating a state where disc radius information is recorded in an address unit (AU) in accordance with the third embodiment of the present invention;

Fig. 12 is a view illustrating the relationship between an encoding system to which an encryption and recording method is applied, and the BD-ROM in accordance with the third embodiment of the present invention;

Fig. 13 is a view illustrating the configuration of an optical disc apparatus to which an encrypted data reproduction method is applied in accordance with an embodiment of the present invention;

Fig. 14 is a flowchart illustrating the encrypted data reproduction method in accordance with the first embodiment of the present invention;

Fig. 15 is a flowchart illustrating the encrypted data reproduction method in accordance with the second embodiment of the present invention; and

Fig. 16 is a flowchart illustrating the encrypted data reproduction method in accordance with the third embodiment of the present invention.

Features, elements, and aspects of the invention that are referenced by the same numerals in different figures represent the same, equivalent, or similar features, elements, or aspects in accordance with one or more embodiments.

5. Modes for Carrying out the Invention

A high-density optical disc, a method for encrypting data and recording the encrypted data thereon, and a method for reproducing the encrypted data recorded thereon in accordance

with preferred embodiments of the present invention will be described in detail with reference to the annexed drawings.

First, as a Blu-ray disc rewritable (BD-RE) 100 in which video data of a moving picture and audio data are discontinuously recorded as shown in Figs. 1 to 6, the high-density optical disc, e.g., a Blu-ray disc-read only memory (BD-ROM), can contain at least one RUB consisting of a run-in area, a physical cluster area, a run-out area and the third guard area (Guard_3). For reference, names of the above-described areas can be changed and designated by other names.

As shown in Fig. 7, the run-in area of the BD-ROM 200 in accordance with the first embodiment of the present invention can include the first guard area (Guard_1) and a preamble area (PrA). The preamble area can contain synchronous data consisting of 24-bit synchronous body data and 6-bit synchronous IDs. The synchronous data recorded in the preamble area of the BD-ROM 200 is different from that recorded in the preamble area of the BD-RE 100.

For example, the first synchronous data (Sync_1) having a synchronous ID of "000 100" and the second synchronous data (Sync_2) having a synchronous ID of "010 000" are sequentially recorded in the preamble area of the BD-RE 100, while the third synchronous data (Sync_3) having a synchronous ID of "000 001" and the second synchronous data (Sync_2) having a synchronous ID of "010 000" are sequentially recorded in the preamble area of the BD-ROM 200.

Further, the third synchronous data (Sync_3) having a synchronous ID of "000 001" is recorded in the post-amble area contained in the run-out area of the BD-RE 100, while the first synchronous data (Sync_1) having a synchronous ID of "000 100" is recorded in the post-amble area contained in the run-out area of the BD-ROM 200 as shown in Fig. 8.

That is, the synchronous data recorded in the preamble or

post-amble area of the BD-ROM 200 is different from that recorded in the preamble or post-amble area of the BD-RE 100.

Encrypted A/V data for preventing unlawful copying can be recorded in the physical cluster area of the BD-ROM 200 containing the synchronous data different from the synchronous data of the BD-RE 100. For example, as shown in Fig. 9, an encoding system 300 recording encrypted data in a physical cluster area of the BD-ROM 200 encrypts A/V data using the third synchronous data or the second and third synchronous data and then records the encrypted A/V data in the physical cluster area.

In accordance with the second embodiment of the present invention, the physical cluster area contained in the RUB of the BD-ROM 200 includes address unit numbers (AUNs) linked to physical sector numbers and physical ADIP addresses. The AUNs recorded on the BD-ROM 200 are different from the AUNs recorded on the BD-RE 100.

For example, the AUNs recorded on the BD-RE 100 have values of "k ~ (k+n)", while the AUNs recorded on the BD-ROM 200 have values of "(k+m) ~ ((k+n)+m)".

That is, the AUNs on the BD-ROM 200 can be recorded to have other values after shifting the values "k ~ (k+n)" of the AUNs on the BD-RE 100 by a predetermined value of "m". Further, the AUNs on the BD-ROM 200 can be recorded to have other values of "s ~ (s+n)" different from the values "k ~ (k+n)" of the AUNs on the BD-RE 100. As a result, the AUNs recorded in the physical cluster area of the BD-ROM 200 are different from the AUNs recorded in the physical cluster area of the BD-RE 100.

In the physical cluster area of the BD-ROM 200 containing the AUNs different from the AUNs recorded in the physical cluster area of the BD-RE 100, encrypted A/V data is recorded to prevent unauthorized or unlawful copying. For example, as shown in Fig. 10, the encoding system 300 recording the encrypted data in the physical cluster area of the BD-ROM 200 encrypts the A/V data using

all or part of AUN information recorded in the physical cluster area, and then records the encrypted A/V data in the physical cluster area.

In accordance with the third embodiment of the present invention, the AU recorded in the physical cluster area can contain disc radius information used for detecting a distance between a criterion of the inner periphery of the BD-ROM 200 and a corresponding position on the disc. For example, the disc radius information can be recorded by the 5^{th} byte of the AU as shown in Fig. 11.

In the physical cluster area of the BD-ROM 200, encrypted A/V data is recorded to prevent unauthorized or unlawful copying. For example, as shown in Fig. 12, the encoding system 300 recording the encrypted data in the physical cluster area of the BD-ROM 200 encrypts the A/V data using the disc radius information recorded in the AU, and then records the encrypted A/V data in the physical cluster area.

For reference, the encoding system 300 can selectively use any conventional encryption processing method such as an encryption method, interleaving method, scrambling method, or etc.

The data is recorded in a discontinuous recording format on the BD-ROM as on the BD-RE. An optical disc apparatus such as a BD-ROM player maintains reproduction compatibility with the BD-RE. The optical disc apparatus performs an encryption and recording operation using each or at least two combination of the synchronous data, AUN and disc radius information, such that unauthorized or unlawful usage of the BD-ROM can be prevented.

Fig. 13 is a view illustrating the configuration of an optical disc apparatus to which an encrypted data reproduction method is applied in accordance with an embodiment of the present invention. An optical disc apparatus, e.g., a BD-ROM player, includes an optical pick-up 2 and data reader 3 for reading

encrypted A/V data discontinuously recorded on a BD-ROM 1; and a reproduction signal processor 4 for decrypting the encrypted A/V data using synchronous data, disc radius information or AU numbers recorded on the BD-ROM 1, decoding the A/V data to original video and audio signals, and processing the video and audio signals to be reproduced.

The BD-ROM player further includes a controller 5 for controlling a reproduction signal processing operation; a buffer 6 for temporarily storing data needed for performing the reproduction signal processing operation, etc.

Fig. 14 is a flowchart illustrating the encrypted data reproduction method in accordance with the first embodiment of the present invention.

When the BD-ROM 1, on which encrypted A/V data is discontinuously recorded as shown in Figs. 7 to 9, is inserted and loaded at step S10, the controller 5 searches for and confirms a lead-in area contained in the BD-ROM 1. The optical disc apparatus reads management information recorded in the lead-in area, i.e., management information for controlling the reproduction of data recorded on the BD-ROM 1, and then stores the read management information in an internal memory (not shown) at step S11.

When the reproduction operation is requested from the user at step S12, the controller 5 performs a sequence of reproduction operations for reading and reproducing the recorded data after moving the optical pick-up 2 to a position where real-time data such as A/V data was first recorded at step S13.

When the run-in area within the RUB shown in Fig. 7 is reproduced while the reproduction operation is performed, the controller 5 searches for and reads synchronous data recorded in the preamble (PrA) area of the run-in area, i.e., the third synchronous data (Sync_3) and/or the second synchronous data (Sync_2) different from the synchronous data recorded on the

BD-RE at step S15.

Then, real-time data, i.e., A/V data encrypted and recorded in the physical cluster area subsequent to the run-in area, is decrypted to original A/V data using the read synchronous data at step S16. The decryption processing operation uses a decryption method corresponding to an encryption method, an interleaving method, a scrambling method, or etc. used in the above-described encryption processing operation.

At step S17, the controller 5 controls an operation of the reproduction signal processor 4 so that a sequence of reproduction signal processing operations for reproducing the decrypted A/V data to output original video and audio signals through an MPEG decoding operation can be appropriately performed. When a reproduction termination request is received according to the user's key input at step S18, the reproduction operation is terminated.

Fig. 15 is a flowchart illustrating the encrypted data reproduction method in accordance with the second embodiment of the present invention.

When the BD-ROM 1, on which encrypted A/V data is discontinuously recorded as shown in Fig. 10, is inserted and loaded at step S20, the controller 5 searches for and confirms a lead-in area contained in the BD-ROM 1. The optical disc apparatus reads management information recorded in the lead-in area, i.e., management information for controlling the reproduction of data recorded on the BD-ROM 1, and then stores the read management information in an internal memory (not shown) at step S21.

When the reproduction operation is requested from the user at step S22, the controller 5 performs a sequence of reproduction operations for reading and reproducing the recorded data after moving the optical pick-up 2 to a position where real-time data such as A/V data was first recorded at step S23.

When the physical cluster area within the RUB shown in Fig. 10 is reproduced while the reproduction operation is performed, the controller 5 searches for and reads AUN information recorded in an AU within the physical cluster area different from AUN information recorded on the BD-RE at step S25.

Then, real-time data, i.e., A/V data encrypted and recorded in the physical cluster area subsequent to the run-in area, is decrypted to original A/V data using all or part of the read AUN information at step S26. The decryption processing operation uses a decryption processing method corresponding to an encryption method, an interleaving method, a scrambling method, or etc. used in the above-described encryption processing operation.

At step S27, the controller 5 controls an operation of the reproduction signal processor 4 so that a sequence of reproduction signal processing operations for reproducing the decrypted A/V data to output original video and audio signals through an MPEG decoding operation can be appropriately performed. When a reproduction termination request is received according to the user's key input at step S28, the reproduction operation is terminated.

Fig. 16 is a flowchart illustrating the encrypted data reproduction method in accordance with the third embodiment of the present invention.

When the BD-ROM 1, on which encrypted A/V data is discontinuously recorded as shown in Figs. 11 and 12, is inserted and loaded at step S30, the controller 5 searches for and confirms a lead-in area contained in the BD-ROM 1. The optical disc apparatus reads management information recorded in the lead-in area, i.e., management information for controlling the reproduction of data recorded on the BD-ROM 1, and then stores the read management information in an internal memory (not shown) at step S31.

When the reproduction operation is requested from the user

at step S32, the controller 5 performs a sequence of reproduction operations for reading and reproducing the recorded data after moving the optical pick-up 2 to a position where real-time data such as A/V data was first recorded at step S33.

When the physical cluster area is reproduced while the reproduction operation is performed, the controller 5 searches for and reads disc radius information within an AU recorded in the physical cluster area at step S35.

Then, real-time data, i.e., A/V data, is decrypted to original A/V data using the read disc radius information at step S36. The decryption processing operation uses a decryption method corresponding to an encryption method, an interleaving method, a scrambling method, or etc. used in the above-described encryption processing operation.

At step S37, the controller 5 controls an operation of the reproduction signal processor 4 so that a sequence of reproduction signal processing operations for reproducing the decrypted A/V data to output original video and audio signals through an MPEG decoding operation can be appropriately performed. When a reproduction termination request is received according to the user's key input at step S38, the reproduction operation is terminated.

The controller 5 searches for and reads the synchronous data, AUN information and disc radius information, and then can perform the decryption processing operation through at least two combinations of the read synchronous data, AUN information and disc radius information.

As described above, the encrypted data is decrypted using synchronous data recorded in the run-in area of the BD-ROM or using the radius information or AUN information recorded in the physical cluster area of the BD-ROM, and the decrypted data is reproduced and processed. Thus, a user holding the optical disc apparatus such as the BD-RE player can be prevented from

unlawfully copying data of the BD-ROM to the BD-RE and unlawfully reproducing the copied data.

For reference, the above-described method for encrypting, decrypting data using the synchronous data, disc radius information or AUN information can be applied to the rewritable optical disc such as the BD-RE.

Further, in accordance with the embodiment of the present invention, the encryption and decryption processing operations for the BD-ROM can be performed on the basis of an arrangement sequence of the existing BD-RE without differentiating the arrangement of the synchronous data items or AUNs on the BD-ROM from that of the synchronous data items or AUNs on the BD-RE.

The preferred embodiments of the present invention have been disclosed for illustrative purposes. Those skilled in the art can readily understand that the present invention can be applied for other high-density optical discs as well as the BD-ROM. Further, those skilled in the art will appreciate that various modifications, additions and substitutions are possible, without departing from the scope and spirit of the invention as disclosed in the accompanying claims.

As apparent from the above description, the present invention provides a high-density optical disc, a method for encrypting data and recording the encrypted data thereon, and a method for reproducing the encrypted data recorded thereon, which can maintain reproduction compatibility with a high-density rewritable optical disc such as a BD-RE in an optical disc apparatus such as a BD-ROM player, and can prevent a user holding an optical disc apparatus such as a BD-RE recorder, etc. from unlawfully copying data recorded on the high-density optical disc and reproducing the copied data.